

Rec'd PCT/PTO 07 FEB 2005

CT/JP03/10186

日本国特許庁
JAPAN PATENT OFFICE

08.08.03

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 2002年 8月 8日
Date of Application:

出願番号 特願2002-231284
Application Number:
[ST. 10/C]: [JP 2002-231284]

出願人 松下電器産業株式会社
Applicant(s):

REC'D 26 SEP 2003

WIPO PCT

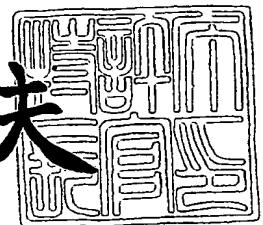
BEST AVAILABLE COPY

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2003年 9月11日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫



出証番号 出証特2003-307449

【書類名】 特許願

【整理番号】 2037830120

【提出日】 平成14年 8月 8日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/00

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 福岡 俊彦

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下システムテクノ株式会社内

【氏名】 和田 妙美

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100077931

【弁理士】

【氏名又は名称】 前田 弘

【選任した代理人】

【識別番号】 100094134

【弁理士】

【氏名又は名称】 小山 廣毅

【選任した代理人】

【識別番号】 100110939

【弁理士】

【氏名又は名称】 竹内 宏

【選任した代理人】

【識別番号】 100110940

【弁理士】

【氏名又は名称】 嶋田 高久

【選任した代理人】

【識別番号】 100113262

【弁理士】

【氏名又は名称】 竹内 祐二

【選任した代理人】

【識別番号】 100115059

【弁理士】

【氏名又は名称】 今江 克実

【選任した代理人】

【識別番号】 100115510

【弁理士】

【氏名又は名称】 手島 勝

【選任した代理人】

【識別番号】 100115691

【弁理士】

【氏名又は名称】 藤田 篤史

【手数料の表示】

【予納台帳番号】 014409

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0006010

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号化復号化装置及び方法、暗号化装置及び方法、並びに復号化装置及び方法

【特許請求の範囲】

【請求項 1】 暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を T E K (traffic encryption key) 制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記 T E K 制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する暗号モード共用処理ブロックとを備え、

前記暗号モード共用処理ブロックは、

入力された鍵データを用いた E C B (electronic code book) 処理を行うことによって、C B C (cipher block chaining) モード及び C F B (cipher feedback) モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化又は復号化を行うものである

暗号化復号化装置。

【請求項 2】 請求項 1 に記載の暗号化復号化装置において、

前記データ構造解析ブロックは、

前記ダウンストリームデータにおける M P E G (moving picture experts group) 構造中のヘッダの解析を行い、前記ヘッダの情報に基づいて前記 M P E G 構造から M A C (media access control) 構造を抜き出し、前記 M A C 構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該ダウンストリームデータが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に

関する情報を前記 T E K 制御用データとして出力するとともに、前記 M A C 構造データから前記拡張ヘッダを除去して前記処理ブロック入力データとして出力するものである

ことを特徴とする暗号化復号化装置。

【請求項 3】 請求項 1 に記載の暗号化復号化装置において、

前記データ制御ブロックは、

前記 T E K 制御用データに従って、前記処理ブロック入力データを C B C モード、及び C F B モードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示す信号を前記モード選択信号として出力するものである

ことを特徴とする暗号化復号化装置。

【請求項 4】 請求項 1 に記載の暗号化復号化装置において、

前記暗号モード共用処理ブロックは、

前記 E C B 処理を行い、得られた結果を暗号処理データとして出力する E C B 処理器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第 1 のセレクトと、

前記処理ブロック入力データ、及び前記暗号処理データを入力とし、それぞれを遅延させて出力する遅延器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延器が出力する遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択して出力する第 2 のセレクトと、

前記第 1 のセレクトの出力と前記第 2 のセレクトの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択して出

力する第3のセレクトと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果として出力する第4のセレクトとを備え、

前記ECB処理器は、

前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記ECB処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第3のセレクトの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする暗号化復号化装置。

【請求項5】 請求項4に記載の暗号化復号化装置において、

前記ビットマスク器は、

前記モード選択信号が56ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとして出力するものである

ことを特徴とする暗号化復号化装置。

【請求項6】 請求項4に記載の暗号化復号化装置において、

前記第1のセレクトは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、その他の場合には、前記暗号処理データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

【請求項7】 請求項4に記載の暗号化復号化装置において、

前記第2のセレクトは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、処

理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC F Bモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC B Cモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC F Bモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力するものである

ことを特徴とする暗号化復号化装置。

【請求項 8】 請求項 4 に記載の暗号化復号化装置において、

前記第 3 のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC B Cモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC F Bモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC B Cモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC F Bモードであることを示す場合には、処

理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択して出力するものであることを特徴とする暗号化復号化装置。

【請求項 9】 請求項 4 に記載の暗号化復号化装置において、
前記第 4 のセレクタは、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号が C B C モードであることを示す場合には、前記暗号処理データを選択して出力し、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号が C F B モードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合には、前記排他的論理和演算器の出力を選択して出力するものであることを特徴とする暗号化復号化装置。

【請求項 10】 請求項 4 に記載の暗号化復号化装置において、
前記 E C B 処理器は、

前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合には、暗号化処理を行い、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号が C B C モードであることを示す場合には、復号化処理を行い、

前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号が C F B モードであることを示す場合には、暗号化処理を行うものである

ことを特徴とする暗号化復号化装置。

【請求項 11】 暗号化データを含むダウンストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報を T E K 制御用データとして出力するとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記 T E K 制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

前記処理ブロック入力データに対して暗号化を行い、得られた暗号化結果を出力する暗号モード共用処理ブロックとを備え、

前記暗号モード共用処理ブロックは、

入力された鍵データを用いた E C B 処理を行うことによって、C B C モード及び C F B モードのいずれにおいても暗号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化を行うものである暗号化装置。

【請求項 12】 請求項 11 に記載の暗号化装置において、

前記暗号モード共用処理ブロックは、

前記 E C B 処理を行い、得られた結果を暗号処理データとして出力する E C B 処理器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第 1 のセレクトと、

前記暗号処理データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した暗号処理データのうちのいずれかを選択して出力する第 2 のセレクトと、

前記第 1 のセレクトの出力と前記第 2 のセレクトの出力との排他的論理和を求めて出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第 3 のセレクトと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、

前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果として出力する第 4 のセレクトとを備え、

前記 E C B 処理器は、

前記 E C B 処理として暗号化処理を前記モードに適合した鍵データを用いて前記第 3 のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする暗号化装置。

【請求項 13】 暗号化すべきデータを含むアップストリームデータを受け取り、そのデータ構造の解析を行って、T E K 制御用データを出力するとともに、前記暗号化すべきデータを前記処理ブロック入力データとして出力するデータ構造解析ブロックと、

前記 T E K 制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、

前記処理ブロック入力データに対して復号化を行い、得られた復号化結果を出力する暗号モード共用処理ブロックとを備え、

前記暗号モード共用処理ブロックは、

入力された鍵データを用いた E C B 処理を行うことによって、C B C モード及び C F B モードのいずれにおいても復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで復号化を行うものである

復号化装置。

【請求項 14】 請求項 13 に記載の復号化装置において、

前記暗号モード共用処理ブロックは、

前記 E C B 処理を行い、得られた結果を暗号処理データとして出力する E C B 処理器と、

前記処理ブロック入力データを入力とし、これを遅延させて出力する遅延器と、

前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した処理ブロック入力データのうちのいずれかを選択して出力する第 2 のセレクタと、

前記暗号処理データと前記第 2 のセレクタの出力との排他的論理和を求めて、前記復号化結果として出力する排他的論理和演算器と、

前記モード選択信号に従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択して出力する第3のセレクタと、

前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器とを備え、

前記ECB処理器は、

前記モード選択信号に従って、前記ECB処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第3のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである

ことを特徴とする復号化装置。

【請求項15】 暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータのデータ構造の解析を行って、暗号化に関する情報をTEK制御用データとして求めるとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして求めるデータ構造解析ステップと、

前記TEK制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替えデータと、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データとを求めるデータ制御ステップと、

前記処理ブロック入力データに対して前記暗号化／復号化切り替えデータに従って暗号化又は復号化を行って、暗号化結果又は復号化結果を求める暗号モード共用処理ステップとを備え、

前記暗号モード共用処理ステップは、

鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化及び復号化を行うものであり、前記モード選択データに示されたモードで暗号化又は復号化を行うものである

暗号化復号化方法。

【請求項16】 請求項15に記載の暗号化復号化方法において、

前記データ構造解析ステップは、

前記ダウンストリームデータにおけるMPEG構造中のヘッダの解析を行い、前記ヘッダの情報に基づいて前記MPEG構造からMAC構造を抜き出し、前記MAC構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該ダウンストリームデータが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に関する情報を前記TEK制御用データとして出力するとともに、前記MAC構造データから拡張ヘッダを除去して前記処理ブロック入力データとして求めるものである

ことを特徴とする暗号化復号化方法。

【請求項17】 請求項15に記載の暗号化復号化方法において、

前記データ制御ステップは、

前記TEK制御用データに従って、前記処理ブロック入力データをCBCモード、及びCFBモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示すデータを前記モード選択データとして求めるものである

ことを特徴とする暗号化復号化方法。

【請求項18】 請求項15に記載の暗号化復号化方法において、

前記暗号モード共用処理ステップは、

前記ECB処理を行い、得られた結果を暗号処理データとするECB処理ステップと、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択する第1の選択ステップと、

前記処理ブロック入力データ、及び前記暗号処理データのそれぞれを遅延させる遅延ステップと、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延ステップで得られた遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択する第2の選択ステップと、

前記第 1 の選択ステップで選択されたデータと前記第 2 の選択ステップで選択されたデータとの排他的論理和を求める排他的論理和演算ステップと、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、前記排他的論理和、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択する第 3 の選択ステップと、

前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップと、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記暗号処理データ及び前記排他的論理和のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果とする第 4 の選択ステップとを備え、

前記 E C B 処理ステップは、

前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記 E C B 処理として暗号化処理及び復号化処理のうちのいずれかを、前記モードに適合した鍵データを用いて前記第 3 の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものであることを特徴とする暗号化復号化方法。

【請求項 19】 請求項 18 に記載の暗号化復号化方法において、

前記ビットマスクステップは、

前記モード選択データが 56 ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとするものであることを特徴とする暗号化復号化方法。

【請求項 20】 請求項 18 に記載の暗号化復号化方法において、

前記第 1 の選択ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データが C B C モードであることを示す場合には、前記処理ブロック入力データを選択し、その他の場合には、前記暗号処理データを選択するものである

ことを特徴とする暗号化復号化方法。

【請求項 21】 請求項 18 に記載の暗号化復号化方法において、

前記第 2 の選択ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データが C B C モードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択し、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データが C F B モードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データが C B C モードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データが C F B モードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択するものである

ことを特徴とする暗号化復号化方法。

【請求項 22】 請求項 18 に記載の暗号化復号化方法において、

前記第 3 の選択ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データが C B C モードであることを示す場合には、前記排他的論理和を選択し、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データが C F B モードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがCBCモードであることを示す場合には、前記処理ブロック入力データを選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがCFBモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択するものである

ことを特徴とする暗号化復号化方法。

【請求項 23】 請求項 18 に記載の暗号化復号化方法において、

前記第 4 の選択ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがCBCモードであることを示す場合には、前記暗号処理データを選択し、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがCFBモードであることを示す場合には、前記排他的論理和を選択し、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合には、前記排他的論理和を選択するものである

ことを特徴とする暗号化復号化方法。

【請求項 24】 請求項 18 に記載の暗号化復号化方法において、

前記 ECB 処理ステップは、

前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合には、暗号化処理を行い、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがCBCモードであることを示す場合には、復号化処理を行い、

前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがCFBモードであることを示す場合には、暗号化処理を行うものである

ことを特徴とする暗号化復号化方法。

【請求項 25】 暗号化データを含むダウンストリームデータのデータ構造の解析を行って、暗号化に関する情報を TEK 制御用データとして求めるとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ステップと、

前記 TEK 制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めるデータ制御ステップと、

前記処理ブロック入力データに対して暗号化を行って、暗号化結果を求める暗号モード共用処理ステップとを備え、

前記暗号モード共用処理ステップは、

鍵データを用いた ECB 処理を行うことによって、CBC モード及び CFB モードのいずれにおいても暗号化を行うことができるものであり、前記モード選択データに示されたモードで暗号化を行うものである暗号化方法。

【請求項 26】 請求項 25 に記載の暗号化方法において、

前記暗号モード共用処理ステップは、

前記 ECB 処理を行い、得られた結果を暗号処理データとする ECB 処理ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択する第 1 の選択ステップと、

前記暗号処理データを遅延させる遅延ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延ステップで得られた遅延した暗号処理データのうちのいずれかを選択する第 2 の選択ステップと、

前記第 1 の選択ステップで選択されたデータと前記第 2 の選択ステップで選択されたデータとの排他的論理和を求める排他的論理和演算ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、前記排他的論理和、及び前記遅延した暗号処理データのうちのいずれかを選択する第 3 の選択ステップと、

前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップと、

前記モード選択データに従って、前記暗号処理データ及び前記排他的論理和のうちのいずれかを選択して、前記暗号化結果とする第 4 の選択ステップとを備え、

前記 E C B 処理ステップは、

前記 E C B 処理として暗号化処理を前記モードに適合した鍵データを用いて前記第 3 の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものであることを特徴とする暗号化方法。

【請求項 2 7】 暗号化すべきデータを含むアップストリームデータのデータ構造の解析を行って、T E K 制御用データとして求めるとともに、前記暗号化すべきデータを前記処理ブロック入力データとして求めるデータ構造解析ステップと、

前記 T E K 制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めて出力するデータ制御ステップと、

前記処理ブロック入力データに対して復号化を行って、復号化結果を求める暗号モード共用処理ステップとを備え、

前記暗号モード共用処理ステップは、

鍵データを用いた E C B 処理を行うことによって、C B C モード及び C F B モードのいずれにおいても復号化を行うことができるものであり、前記モード選択データに示されたモードで復号化を行うものである復号化方法。

【請求項 2 8】 請求項 2 7 に記載の復号化方法において、

前記暗号モード共用処理ステップは、

前記 E C B 処理を行い、得られた結果を暗号処理データとする E C B 処理ステップと、

前記処理ブロック入力データを遅延させる遅延ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延ステップで得られた遅延した処理ブロック入力データのうちのいずれかを選択する第 2 の選択ステップと、

前記暗号処理データと前記第 2 の選択ステップで選択されたデータとの排他的論理和を求めて、前記復号化結果とする排他的論理和演算ステップと、

前記モード選択データに従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択する第 3 の選択ステップと

、
前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップとを備え

、
前記 E C B 処理ステップは、

前記モード選択データに従って、前記 E C B 処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第 3 の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである

ことを特徴とする復号化方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、暗号化及び暗号の復号化技術に関する。

【 0 0 0 2 】

【従来の技術】

デジタル双方向通信の代表的な例である双方向 C A T V (cable television) システムでは、暗号化機能を実現するために、T V 端末には暗号化機能が実装される。この暗号化機能としては、D E S (data encryption standard) 暗号に代表される秘密鍵暗号方式と、R S A (Rivest-Shamir-Adleman) 暗号に代表される公開鍵暗号方式とを組み合わせた方式が用いられる。

【 0 0 0 3 】

秘密鍵暗号方式とは、暗号化と復号化とに用いる鍵が共通であり、暗号化に用いられた鍵を用いて暗号化アルゴリズムを逆の順に実行することによって復号化を行い、暗号化を施す前の原文を得る方式である。この方式は、単純な排他的論理和の繰り返しアルゴリズムで実現されるもので、高速な処理を可能とする反面、送信側と受信側とで共通の鍵を保有する必要がある、鍵の配送・保持が困難であるという特徴を有する。

【0 0 0 4】

公開鍵暗号方式とは、落とし戸関数と呼ばれる、関数の演算は容易に実行でき、逆関数の演算を行うのは非常に困難であるような関数を利用するものであり、暗号化と復号化とに使用する鍵が異なるものである。したがって、鍵の配送・保持は容易に行える反面、秘密鍵暗号方式に比べて計算が複雑であり、秘密鍵暗号方式と比較して暗号化・復号化により多くの処理時間を要する。ただし、公開鍵暗号方式を使用して認証及び鍵配送を行い、秘密鍵暗号方式を使用してデータの暗号化を行うことによって、それぞれの利点を生かすことが可能となる。

【0 0 0 5】

さて、米国の標準方式である D E S 暗号方式では、E C B (electronic code book) モードと呼ばれる、入力データサイズが 6 4 ビット、出力データサイズが 6 4 ビットの演算を基本処理として行う。この暗号方式の暗号化アルゴリズムに対して、あらかじめ文字又は単語が出現する頻度の分布を統計処理しておけば、入手した暗号化文の文字列パターンの頻度分布とのマッチングをとることにより、暗号化前の平文が推定されてしまう可能性がある。

【0 0 0 6】

そこで、暗号化された 6 4 ビットの暗号ブロックと次に入力される 6 4 ビットの入力データとの排他的論理和を演算して暗号文を作成する方法が考え出された。この方法を行って暗号化するモードを C B C (cipher block chaining) モードと呼んでいる。また、パケット通信のように通信を行う際のデータ単位があらかじめ決められている場合があるが、6 4 ビットを 1 ブロックとするブロック暗号化方式では、1 ブロックのビット数 (6 4 ビット) で割り切れないデータ単位が入力された場合には、1 ブロックに満たない端数データができる。

【0 0 0 7】

データに端数部分がある場合には、1つ前のブロックの暗号解読演算結果と端数データの排他的論理和演算を実行し暗号化する。このような端数処理を行うモードの1つとして、C F B (cipher feedback) モードがあり、C F Bモードによって、データが6 4 ビットに満たない場合でも暗号文を得ることができる。

【0 0 0 8】

また、暗号化及び暗号解読（復号化）のいずれの演算においても、通常は5 6 ビットのデータを鍵として用いるが、特定の条件下では、4 0 ビットのデータを鍵として用いるモードも存在する。この場合、他のモードの場合と同様に、演算処理自体は6 4 ビット単位で行うが、鍵の有効データが4 0 ビットとなる。

【0 0 0 9】

このように、秘密鍵暗号方式演算においては複数のモード、すなわち、E C B モード、C B C モード及びC F B モードのうちの1つと、5 6 ビット鍵モード又は4 0 ビット鍵モードのいずれかとの組み合わせに対応したモードが存在する。そして、デジタル双方向通信のセキュリティ機能を実現するために、すべてのモードに対応した暗号化装置又は復号化装置が一般的に用いられる。

【0 0 1 0】**【発明が解決しようとする課題】**

従来のD E S 暗号方式に基づく暗号化装置又は復号化装置は、複数のモードのそれぞれのための回路を備え、システムの要求に応じて複数のモードのいずれかを適宜選択し、そのモードのための回路を用いて暗号化演算又は暗号解読演算を行う構成となっている。

【0 0 1 1】

ところが、近年、暗号化又は暗号解読を必要とするシステムでは、単一の鍵のみを使用する場合は少なく、複数の鍵を使用して、それぞれの鍵に対応した演算を行う場合も増加してきている。

【0 0 1 2】

これを実現する装置は、各モードごとの暗号化又は暗号解読機能を備えた上、複数の鍵に対する演算を行う機能も必須となり、回路規模は莫大なものとなる。

一般的に、複数の鍵に対する演算は並列実行する必要があるため、処理が必要となる鍵の数が増大すると、装置としても、鍵の数に応じた数の処理回路を有する必要がある。

【0013】

しかし、DESの各モードは、ECB処理と呼ばれる、DESの基本処理を変形した処理が行われるものである。また、各モードを同時に並列実行する場合はほとんどない。このため、暗号化装置及び復号化装置において、複数のモードで処理回路を共用化して回路規模を削減することは可能である。

【0014】

本発明は、複数のモードで処理回路を共用化することによって、回路規模を削減した暗号化復号化装置、暗号化装置、及び復号化装置を提供することを目的とする。

【0015】

【課題を解決するための手段】

前記課題を解決するため、請求項1の発明が講じた手段は、暗号化復号化装置として、暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報をTEK (traffic encryption key) 制御用データとして出力するとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記TEK制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号と、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号とを出力するデータ制御ブロックと、前記処理ブロック入力データに対して前記暗号化／復号化切り替え信号に従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を出力する暗号モード共用処理ブロックとを備え、前記暗号モード共用処理ブロックは、入力された鍵データを用いたECB (electronic code book) 処理を行うことによって、CBC (cipher block chaining) モード及びCFB (cipher feedback) モードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、前記モード選択信号に示され

たモードで暗号化又は復号化を行うものである。

【0016】

請求項1の発明によると、CBCモード又はCFBモードのいずれのモードにおいても、同一のハードウェアによって暗号化及び復号化を行うことができる。したがって、暗号化復号化装置の回路規模を抑えることができる。

【0017】

また、請求項2の発明では、請求項1に記載の暗号化復号化装置において、前記データ構造解析ブロックは、前記ダウンストリームデータにおけるMPEG（moving picture experts group）構造中のヘッダの解析を行い、前記ヘッダの情報に基づいて前記MPEG構造からMAC（media access control）構造を抜き出し、前記MAC構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該ダウンストリームデータが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に関する情報を前記TEK制御用データとして出力するとともに、前記MAC構造データから前記拡張ヘッダを除去して前記処理ブロック入力データとして出力するものである。

【0018】

また、請求項3の発明では、請求項1に記載の暗号化復号化装置において、前記データ制御ブロックは、前記TEK制御用データに従って、前記処理ブロック入力データをCBCモード、及びCFBモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示す信号を前記モード選択信号として出力するものである。

【0019】

また、請求項4の発明では、請求項1に記載の暗号化復号化装置において、前記暗号モード共用処理ブロックは、前記ECB処理を行い、得られた結果を暗号処理データとして出力するECB処理器と、前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第1のセレクタと、前記処理ブロック入力データ、及び前記暗号処理データを入力とし、それぞれを遅延させて出力する遅延器と、前記暗号化／復号化切り替え信号及び前記モード選択信号に従

って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延器が出力する遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択して出力する第2のセレクタと、前記第1のセレクタの出力と前記第2のセレクタの出力との排他的論理和を求めて出力する排他的論理和演算器と、前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第3のセレクタと、前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果として出力する第4のセレクタとを備え、前記ECB処理器は、前記暗号化／復号化切り替え信号及び前記モード選択信号に従って、前記ECB処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第3のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである。

【0020】

請求項4の発明によると、複数のモードにおいて暗号化及び復号化を行うことが、セレクタ等の簡単な回路を用いることによって実現できる。

【0021】

また、請求項5の発明では、請求項4に記載の暗号化復号化装置において、前記ビットマスク器は、前記モード選択信号が56ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとして出力するものである。

【0022】

また、請求項6の発明では、請求項4に記載の暗号化復号化装置において、前記第1のセレクタは、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、その他の場合

には、前記暗号処理データを選択して出力するものである。

【0023】

また、請求項7の発明では、請求項4に記載の暗号化復号化装置において、前記第2のセレクトは、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択して出力し、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCFBモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した処理ブロック入力データを選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCFBモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択して出力するものである。

【0024】

また、請求項8の発明では、請求項4に記載の暗号化復号化装置において、前記第3のセレクトは、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCFBモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がCBCモードであることを示す場合には、前記処理ブロック入力データを選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択

信号がC F Bモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択して出力するものである。

【0025】

また、請求項9の発明では、請求項4に記載の暗号化復号化装置において、前記第4のセレクトは、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC B Cモードであることを示す場合には、前記暗号処理データを選択して出力し、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC F Bモードであることを示す場合には、前記排他的論理和演算器の出力を選択して出力し、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合には、前記排他的論理和演算器の出力を選択して出力するものである。

【0026】

また、請求項10の発明では、請求項4に記載の暗号化復号化装置において、前記E C B処理器は、前記暗号化／復号化切り替え信号が暗号化をすべきであることを示す場合には、暗号化処理を行い、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC B Cモードであることを示す場合には、復号化処理を行い、前記暗号化／復号化切り替え信号が復号化をすべきであることを示す場合であって、かつ、前記モード選択信号がC F Bモードであることを示す場合には、暗号化処理を行うものである。

【0027】

また、請求項11の発明は、暗号化装置として、暗号化データを含むダウンストリームデータを受け取り、そのデータ構造の解析を行って、暗号化に関する情報をT E K制御用データとして出力するとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ブロックと、前記T E K制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、前記処理ブロック入力デ

ータに対して暗号化を行い、得られた暗号化結果を出力する暗号モード共用処理ブロックとを備え、前記暗号モード共用処理ブロックは、入力された鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化を行うことができるように構成されており、前記モード選択信号に示されたモードで暗号化を行うものである。

【0028】

請求項11の発明によると、CBCモード又はCFBモードのいずれのモードにおいても、同一のハードウェアによって暗号化を行うことができる。したがって、暗号化装置の回路規模を抑えることができる。

【0029】

また、請求項12の発明では、請求項11に記載の暗号化装置において、前記暗号モード共用処理ブロックは、前記ECB処理を行い、得られた結果を暗号処理データとして出力するECB処理器と、前記モード選択信号に従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択して出力する第1のセレクトと、前記暗号処理データを入力とし、これを遅延させて出力する遅延器と、前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した暗号処理データのうちのいずれかを選択して出力する第2のセレクトと、前記第1のセレクトの出力と前記第2のセレクトの出力との排他的論理和を求めて出力する排他的論理和演算器と、前記モード選択信号に従って、前記処理ブロック入力データ、前記排他的論理和演算器の出力、及び前記遅延した暗号処理データのうちのいずれかを選択して出力する第3のセレクトと、前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器と、前記モード選択信号に従って、前記暗号処理データ及び前記排他的論理和演算器の出力のうちのいずれかを選択して、前記暗号化結果として出力する第4のセレクトとを備え、前記ECB処理器は、前記ECB処理として暗号化処理を前記モードに適合した鍵データを用いて前記第3のセレクトの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである。

【0030】

請求項12の発明によると、複数のモードにおいて暗号化を行うことが、セクタ等の簡単な回路を用いることによって実現できる。

【0031】

また、請求項13の発明は、復号化装置として、暗号化すべきデータを含むアップストリームデータを受け取り、そのデータ構造の解析を行って、TEK制御用データを出力するとともに、前記暗号化すべきデータを前記処理ブロック入力データとして出力するデータ構造解析ブロックと、前記TEK制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択信号を出力するデータ制御ブロックと、前記処理ブロック入力データに対して復号化を行い、得られた復号化結果を出力する暗号モード共用処理ブロックとを備え、前記暗号モード共用処理ブロックは、入力された鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても復号化を行うことができるように構成されており、前記モード選択信号に示されたモードで復号化を行うものである。

【0032】

請求項13の発明によると、CBCモード又はCFBモードのいずれのモードにおいても、同一のハードウェアによって復号化を行うことができる。したがって、復号化装置の回路規模を抑えることができる。

【0033】

また、請求項14の発明では、請求項13に記載の復号化装置において、前記暗号モード共用処理ブロックは、前記ECB処理を行い、得られた結果を暗号処理データとして出力するECB処理器と、前記処理ブロック入力データを入力とし、これを遅延させて出力する遅延器と、前記モード選択信号に従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延器が出力する遅延した処理ブロック入力データのうちのいずれかを選択して出力する第2のセクタと、前記暗号処理データと前記第2のセクタの出力との排他的論理和を求めて、前記復号化結果として出力する排他的論理和演算器と、前記モード選択信号に従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力デ

ータのうちのいずれかを選択して出力する第3のセレクタと、前記鍵データを、前記モード選択信号に従って必要に応じてその一部をマスクして、モードに適合した鍵データとして出力するビットマスク器とを備え、前記ECB処理器は、前記モード選択信号に従って、前記ECB処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第3のセレクタの出力に対して行い、得られた結果を前記暗号処理データとして出力するものである。

【0034】

請求項14の発明によると、複数のモードにおいて復号化を行うことが、セレクタ等の簡単な回路を用いることによって実現できる。

【0035】

また、請求項15の発明は、暗号化復号化方法として、暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータのデータ構造の解析を行って、暗号化に関する情報をTEK制御用データとして求めるとともに、前記暗号化データ又は前記暗号化すべきデータを処理ブロック入力データとして求めるデータ構造解析ステップと、前記TEK制御用データに従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替えデータと、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データとを求めるデータ制御ステップと、前記処理ブロック入力データに対して前記暗号化／復号化切り替えデータに従って暗号化又は復号化を行って、暗号化結果又は復号化結果を求める暗号モード共用処理ステップとを備え、前記暗号モード共用処理ステップは、鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化及び復号化を行うものであり、前記モード選択データに示されたモードで暗号化又は復号化を行うものである。

【0036】

また、請求項16の発明では、請求項15に記載の暗号化復号化方法において、前記データ構造解析ステップは、前記ダウンストリームデータにおけるMP EG構造中のヘッダの解析を行い、前記ヘッダの情報に基づいて前記MP EG構造

からMAC構造を抜き出し、前記MAC構造中に拡張ヘッダが存在し、かつ、前記拡張ヘッダに当該ダウンストリームデータが暗号化されていることが示されている場合には、前記拡張ヘッダに含まれる暗号化に関する情報を前記TEK制御用データとして出力するとともに、前記MAC構造データから拡張ヘッダを除去して前記処理ブロック入力データとして求めるものである。

【0037】

また、請求項17の発明では、請求項15に記載の暗号化復号化方法において、前記データ制御ステップは、前記TEK制御用データに従って、前記処理ブロック入力データをCBCモード、及びCFBモードのうちのいずれのモードで処理すべきか、並びにいずれの長さの鍵データを用いるモードで処理すべきかを示すデータを前記モード選択データとして求めるものである。

【0038】

また、請求項18の発明では、請求項15に記載の暗号化復号化方法において、前記暗号モード共用処理ステップは、前記ECB処理を行い、得られた結果を暗号処理データとするECB処理ステップと、前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択する第1の選択ステップと、前記処理ブロック入力データ、及び前記暗号処理データのそれぞれを遅延させる遅延ステップと、前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、並びに、前記遅延ステップで得られた遅延した処理ブロック入力データ及び遅延した暗号処理データのうちのいずれかを選択する第2の選択ステップと、前記第1の選択ステップで選択されたデータと前記第2の選択ステップで選択されたデータとの排他的論理和を求める排他的論理和演算ステップと、前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記処理ブロック入力データ、前記排他的論理和、前記遅延した処理ブロック入力データ、及び前記遅延した暗号処理データのうちのいずれかを選択する第3の選択ステップと、前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップと、前記暗号化／復号化切り替えデータ及

び前記モード選択データに従って、前記暗号処理データ及び前記排他的論理和のうちのいずれかを選択して、前記暗号化結果又は前記復号化結果とする第4の選択ステップとを備え、前記ECB処理ステップは、前記暗号化／復号化切り替えデータ及び前記モード選択データに従って、前記ECB処理として暗号化処理及び復号化処理のうちのいずれかを、前記モードに適合した鍵データを用いて前記第3の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである。

【0039】

また、請求項19の発明では、請求項18に記載の暗号化復号化方法において、前記ビットマスクステップは、前記モード選択データが56ビット鍵モードであることを示す場合には、前記鍵データをそのまま、その他の場合には、必要がないビットをマスクして、前記モードに適合した鍵データとするものである。

【0040】

また、請求項20の発明では、請求項18に記載の暗号化復号化方法において、前記第1の選択ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがCBCモードであることを示す場合には、前記処理ブロック入力データを選択し、その他の場合には、前記暗号処理データを選択するものである。

【0041】

また、請求項21の発明では、請求項18に記載の暗号化復号化方法において、前記第2の選択ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがCBCモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記遅延した暗号処理データを選択し、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがCFBモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがCBCモードであることを示す場合には、処理開始時に前記初期ベクタデ

ータを、その後は前記遅延した処理ブロック入力データを選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがC F Bモードであることを示す場合には、処理開始時に前記初期ベクタデータを、その後は前記処理ブロック入力データを選択するものである。

【0042】

また、請求項22の発明では、請求項18に記載の暗号化復号化方法において、前記第3の選択ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがC B Cモードであることを示す場合には、前記排他的論理和を選択し、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがC F Bモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した暗号処理データを選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがC B Cモードであることを示す場合には、前記処理ブロック入力データを選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データがC F Bモードであることを示す場合には、処理開始時に前記処理ブロック入力データを、その後は前記遅延した処理ブロック入力データを選択するものである。

【0043】

また、請求項23の発明では、請求項18に記載の暗号化復号化方法において、前記第4の選択ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがC B Cモードであることを示す場合には、前記暗号処理データを選択し、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合であって、かつ、前記モード選択データがC F Bモードであることを示す場合には、前記排他的論理和を選択し、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合には、前記排他的論理和を選択するものである。

【0044】

また、請求項 2 4 の発明では、請求項 1 8 に記載の暗号化復号化方法において、前記 E C B 処理ステップは、前記暗号化／復号化切り替えデータが暗号化をすべきであることを示す場合には、暗号化処理を行い、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データが C B C モードであることを示す場合には、復号化処理を行い、前記暗号化／復号化切り替えデータが復号化をすべきであることを示す場合であって、かつ、前記モード選択データが C F B モードであることを示す場合には、暗号化処理を行うものである。

【 0 0 4 5 】

また、請求項 2 5 の発明は、暗号化方法として、暗号化データを含むダウンストリームデータのデータ構造の解析を行って、暗号化に関する情報を T E K 制御用データとして求めるとともに、前記暗号化データを処理ブロック入力データとして出力するデータ構造解析ステップと、前記 T E K 制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めるデータ制御ステップと、前記処理ブロック入力データに対して暗号化を行って、暗号化結果を求める暗号モード共用処理ステップとを備え、前記暗号モード共用処理ステップは、鍵データを用いた E C B 処理を行うことによって、C B C モード及び C F B モードのいずれにおいても暗号化を行うことができるものであり、前記モード選択データに示されたモードで暗号化を行うものである。

【 0 0 4 6 】

また、請求項 2 6 の発明では、請求項 2 5 に記載の暗号化方法において、前記暗号モード共用処理ステップは、前記 E C B 処理を行い、得られた結果を暗号処理データとする E C B 処理ステップと、前記モード選択データに従って、前記処理ブロック入力データ、及び前記暗号処理データのうちのいずれかを選択する第 1 の選択ステップと、前記暗号処理データを遅延させる遅延ステップと、前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延ステップで得られた遅延した暗号処理データのうちのいずれかを選択する第 2 の選択ステップと、前記第 1 の選択ステップで選択されたデータと

前記第2の選択ステップで選択されたデータとの排他的論理和を求める排他的論理和演算ステップと、前記モード選択データに従って、前記処理ブロック入力データ、前記排他的論理和、及び前記遅延した暗号処理データのうちのいずれかを選択する第3の選択ステップと、前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップと、前記モード選択データに従って、前記暗号処理データ及び前記排他的論理和のうちのいずれかを選択して、前記暗号化結果とする第4の選択ステップとを備え、前記ECB処理ステップは、前記ECB処理として暗号化処理を前記モードに適合した鍵データを用いて前記第3の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである。

【0047】

また、請求項27の発明は、復号化方法として、暗号化すべきデータを含むアップストリームデータのデータ構造の解析を行って、TEK制御用データとして求めるとともに、前記暗号化すべきデータを前記処理ブロック入力データとして求めるデータ構造解析ステップと、前記TEK制御用データに従って、前記処理ブロック入力データをいずれのモードで処理すべきかを示すモード選択データを求めて出力するデータ制御ステップと、前記処理ブロック入力データに対して復号化を行って、復号化結果を求める暗号モード共用処理ステップとを備え、前記暗号モード共用処理ステップは、鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても復号化を行うことができるものであり、前記モード選択データに示されたモードで復号化を行うものである。

【0048】

また、請求項28の発明では、請求項27に記載の復号化方法において、前記暗号モード共用処理ステップは、前記ECB処理を行い、得られた結果を暗号処理データとするECB処理ステップと、前記処理ブロック入力データを遅延させる遅延ステップと、前記モード選択データに従って、前記処理ブロック入力データ、前記初期ベクタデータ、及び前記遅延ステップで得られた遅延した処理プロ

ック入力データのうちのいずれかを選択する第2の選択ステップと、前記暗号処理データと前記第2の選択ステップで選択されたデータとの排他的論理和を求めて、前記復号化結果とする排他的論理和演算ステップと、前記モード選択データに従って、前記処理ブロック入力データ、及び前記遅延した処理ブロック入力データのうちのいずれかを選択する第3の選択ステップと、前記鍵データを、前記モード選択データに従って必要に応じてその一部をマスクして、モードに適合した鍵データとして求めるビットマスクステップとを備え、前記ECB処理ステップは、前記モード選択データに従って、前記ECB処理として暗号化処理及び復号化処理のうちのいずれかを前記モードに適合した鍵データを用いて前記第3の選択ステップで選択されたデータに対して行い、得られた結果を前記暗号処理データとするものである。

【0049】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を参照しながら説明する。

【0050】

図1は、本発明の実施形態に係る暗号化復号化装置の構成を示すブロック図である。図1の暗号化復号化装置は、データ構造解析ブロック2と、暗号モード共用処理ブロック4と、データ制御ブロック6とを備えている。図1の暗号化復号化装置は、例えば、センター装置及び複数の端末装置により構成される双方向通信網において、端末装置の1つを構成するものである。センター装置は、暗号化されたデータを含むダウンストリームデータSDを端末装置に送信する。ダウンストリームデータSDには、映像データ及び伝送制御データが含まれている。一方、端末装置は、暗号化すべきデータを含むアップストリームデータを受け取り、暗号化してセンター装置に対して送信する。

【0051】

データ構造解析ブロック2は、ダウンストリームデータSDを受け取り、その構文解析を行う。ダウンストリームデータSDは、例えば、映像データにおけるMP EG構造と、MP EG構造に埋め込まれているネットワーク処理用のサブレイヤであるMAC (media access control) 構造を有している。

【0052】

まず、データ構造解析ブロック 2 は、MPEG 構造データ中のヘッダ部分を解析し、MAC 構造データを抜き出すための情報を抽出した後に、MAC 構造データを抜き出す。次に、MAC 構造データ中のヘッダ部分を解析し、通常のヘッダのみでなく、拡張ヘッダと呼ばれる拡張されたフィールドが存在する場合は、この拡張ヘッダを解析する。拡張ヘッダは、データ構成の拡張を可能にするものであって、暗号化の有無、その他の暗号化又は復号化のための処理に必要となる情報を有している。

【0053】

拡張ヘッダが存在しない場合、データ構造解析ブロック 2 は、ダウンストリームデータ SD が暗号化されていないと判断する。この場合、データ構造解析ブロック 2 は、TEK 制御用データ TK を例えば値 “0” に固定し、データ制御ブロック 6 に出力する。

【0054】

拡張ヘッダが存在する場合、データ構造解析ブロック 2 は、暗号化に関する情報を格納するフィールドを解析する。暗号化されていないことを確認した場合には、拡張ヘッダが存在しない場合と同様の処理を行う。暗号化されていることを確認した場合には、暗号化に関する情報である SID (service ID) 及びキーシーケンスナンバー (key sequence number) を拡張ヘッダから抽出し、TEK 制御用データ TK としてデータ制御ブロック 6 に出力する。

【0055】

また、データ構造解析ブロック 2 は、暗号化すべきデータをアップストリームデータ SU として受け取り、その構文解析を行う。データ構造解析ブロック 2 は、アップストリームデータ SU に含まれるデータから SID 及びキーシーケンスナンバーを抽出し、TEK 制御用データ TK としてデータ制御ブロック 6 に出力する。

【0056】

データ構造解析ブロック 2 は、ダウンストリームデータ SD に含まれる MPEG 構造を有する暗号化データ、又はアップストリームデータ SU に含まれる暗号

化すべきデータを、処理ブロック入力データ EC として暗号モード共用処理ブロック 4 に出力する。

【0057】

データ構造解析ブロック 2 は、受信したダウンストリームデータ SD 又はアップストリームデータ SU のパケットのビット数をカウントし、ストリームのパケットのビット数が 64 ビット以下、64 ビットの倍数、又は 64 ビットの倍数と 64 ビット以下の端数との和のいずれであるか、及びパケットのうち処理ブロック入力データ EC として出力したビット数（パケットカウント）を求める。データ構造解析ブロック 2 は、求められた結果、並びに、ダウンストリームデータ SD を受け取った場合には復号化すべきであることを、及びアップストリームデータ SU を受け取った場合には暗号化すべきであることをも TEK 制御用データ TK としてデータ制御ブロック 6 に出力する。

【0058】

次に、データ制御ブロック 6 は、データ構造解析ブロック 2 から受信した TEK 制御用データ TK を用いて処理を行う。まず、SID 及びキーシーケンスナンバーをチェックして、これらのデータがあらかじめ決められている有効な数値であるかどうかを判断する。無効な数値であると判断した場合は、何も処理を行わない。有効な数値であると判断した場合は、データ制御ブロック 6 は、56 ビット鍵モードであるか否かをチェックする。暗号化及び復号化には、56 ビットの鍵が標準として用いられるが、これ以外の長さの鍵も用いられる。以下では例として、56 ビット又は 40 ビットの鍵が用いられるものとする。56 ビット鍵モードであるか否かは、SID 及びキーシーケンスナンバーに一意に対応する。データ制御ブロック 6 は、56 ビット鍵モードであるか否かを示す情報をモード選択信号 MS として出力する。

【0059】

データ制御ブロック 6 は、TEK 制御用データ TK に従って、暗号化又は復号化のいずれを行うべきかを示す暗号化／復号化切り替え信号 SS を暗号モード共用処理ブロック 4 に出力する。また、データ制御ブロック 6 は、TEK 制御用データ TK を参照して、処理ブロック入力データ EC のパケットのビット数が 64

ビット以下の場合はCFBモードを示す信号を、64ビットの倍数である場合はCBCモードを示す信号を、モード選択信号MSとして暗号モード共用処理ブロック4に出力する。

【0060】

パケットのビット数が64ビットの倍数と64ビット以下の端数との和である場合は、データ制御ブロック6は、パケットカウントに応じて、モード選択信号MSを次のように切り替える。すなわち、データ構造解析ブロック2が64ビットの倍数に相当する処理ブロック入力データECを出力しているときは、CBCモードを示す信号を、64ビット以下の端数に相当する処理ブロック入力データECを出力しているときは、CFBモードを示す信号を、データ制御ブロック6がモード選択信号MSとして出力する。また、データ制御ブロック6は、それぞれのモードの処理を開始する初期状態、又はその後の定常状態のいずれであるかも、モード選択信号MSとして出力する。

【0061】

また、データ構造解析ブロック2は、受信したダウンストリームデータSD又はアップストリームデータSUに応じて、ECBモードで処理すべきか否かをTEK制御用データTKによってデータ制御ブロック6に通知する。ECBモードで処理すべき場合には、データ制御ブロック6は、ECBモードを示す信号をモード選択信号MSとして出力する。

【0062】

このように、データ制御ブロック6は、SID、キーシーケンスナンバー、及びパケットカウント等に応じてモード選択信号MSを切り替えて、暗号モード共用処理ブロック4に出力する。

【0063】

暗号モード共用処理ブロック4は、外部から入力された初期ベクタデータIV、及び鍵データKDを用いたECB処理を行うことによって、ECBモード、CBCモード及びCFBモードのいずれにおいても、処理ブロック入力データECに対して暗号化及び復号化を行うことができるように構成されている。暗号モード共用処理ブロック4は、モード選択信号MSに示されたモードで、暗号化／復

号化切り替え信号SSに従って暗号化又は復号化を行い、得られた暗号化結果又は復号化結果を処理済データDCとして出力する。

【0064】

図2は、図1の暗号モード共用処理ブロック4の構成の例を示すブロック図である。図2の暗号モード共用処理ブロック4は、第1のセクタ41と、第2のセクタ42と、第3のセクタ43と、第4のセクタ44と、ビットマスク器46と、ECB処理器47と、遅延器48と、排他的論理和演算器49とを備えている。

【0065】

第1のセクタ41は、暗号化／復号化切り替え信号SS及びモード選択信号MSに従って、処理ブロック入力データEC、及びECB処理器47が出力する暗号処理データPDのうちのいずれかを選択して排他的論理和演算器49に出力する。

【0066】

遅延器48は、処理ブロック入力データEC、及び暗号処理データPDを入力とし、それぞれを、ECB処理器47が64ビットのデータに対してECB処理を行うのに要する時間だけ遅延させて、第2のセクタ42に出力する。

【0067】

第2のセクタ42は、暗号化／復号化切り替え信号SS及びモード選択信号MSに従って、処理ブロック入力データEC、初期ベクタデータIV、並びに、遅延器48が出力する遅延した処理ブロック入力データECD及び遅延した暗号処理データPDDのうちのいずれかを選択して排他的論理和演算器49に出力する。

【0068】

排他的論理和演算器49は、第1のセクタ41の出力と第2のセクタ42の出力との排他的論理和を対応するビット毎に求めて第4のセクタ44に出力する。

【0069】

第3のセクタ43は、暗号化／復号化切り替え信号SS及びモード選択信号

MSに従って、処理ブロック入力データEC、排他的論理和演算器49が出力する排他的論理和データER、遅延した処理ブロック入力データECD、及び遅延した暗号処理データPDDのうちのいずれかを選択してECB処理器47に出力する。

【0070】

ビットマスク器46は、鍵データKDを、モード選択信号MSに従って必要に応じてその一部をマスクして、モードに適合した鍵データとしてECB処理器47に出力する。

【0071】

第4のセクタ44は、暗号化／復号化切り替え信号SS及びモード選択信号MSに従って、暗号処理データPD及び排他的論理和演算器49が出力する排他的論理和データERのうちのいずれかを選択して、暗号化結果又は復号化結果として出力する。

【0072】

ECB処理器47は、暗号化／復号化切り替え信号SS及びモード選択信号MSに従って、ECB処理として暗号化処理及び復号化処理のうちのいずれかを、第3のセクタ43の出力に対して行う。ECB処理器47は、ビットマスク器46が出力するモードに適合した鍵データを用いてECB処理を行い、得られた結果を暗号処理データPDとして第1のセクタ41、第4のセクタ44、及び遅延器48に出力する。

【0073】

図3は、図1の暗号モード共用処理ブロック4が行う処理の流れを示す説明図である。図3において、上段は暗号化処理の流れを示し、下段は復号化処理の流れを示している。処理E1、E2、E3、E9、D1、D2、D3、D9はそれぞれECB処理を表している。暗号モード共用処理ブロック4は、暗号化処理及び復号化処理のいずれの場合にも、CBCモードによる処理を行う必要があるときは、CBCモードによる処理を連続して行い、その後、必要に応じてCFBモードによる処理を行う。

【0074】

図3では、処理E9、D9を含む最も右の列の処理はCFBモードの処理を示している。処理E1、E2、E3、D1、D2、D3を含むその他の3つの列の処理はCBCモードの処理を示している。また、「IV」は初期ベクタデータ、「D」は暗号化されていないデータ、「I」は、図3上段の暗号化処理の場合はECB処理前、下段の復号化処理の場合はECB処理後のデータを示す。また、「C」は暗号化データ、「Encrypt」はECB処理器47におけるECB処理が暗号化処理であること、「Decrypt」はECB処理器47におけるECB処理が復号化処理であることを示す。実際のECB処理には鍵データを用いるが、図3においては、鍵データのデータフローは省略している。図3の処理の流れは、56ビット鍵モードであるか否かにかかわらず同様である。

【0075】

図4は、図1の暗号モード共用処理ブロック4の第1～第4のセレクタ41～44が選択するデータの組み合わせを示す説明図である。暗号モード共用処理ブロック4の復号化処理時の動作について、図2、図3の下段、及び図4を参照して説明する。この場合、暗号モード共用処理ブロック4には、暗号化／復号化切り替え信号SSとして、復号化を示す信号が入力される。56ビット鍵モードであるか否か、CBCモード及びCFBモードのうちのいずれであるか、初期状態及び定常状態のうちのいずれであるかによって場合を分けて説明する。ECB処理器47におけるECB処理は、CBCモードの場合は復号化処理、CFBモードの場合は暗号化処理である。

【0076】

1) 56ビット鍵モードであり、かつ、CBCモードの初期状態である場合（図4のDEC-CBC Initの場合）

この場合は、図3の下段の処理D1及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック4は、暗号化データCを入力とし、ECB処理として「Decrypt」処理を行って、データIを求める。暗号モード共用処理ブロック4は、求められたデータIと入力された初期ベクタデータIVとの排他的論理和を求めて、暗号化されていないデータDとして出力する。

【0077】

この場合の処理を、図2を参照して説明する。暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCBCモードの初期状態であることを示す信号が入力される。

【0078】

第1のセレクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセレクタ42は、初期ベクタデータIVを選択して出力する。排他的論理和演算器49は、暗号処理データPDと初期ベクタデータIVとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

【0079】

第3のセレクタ43は、処理ブロック入力データECを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

【0080】

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセレクタから出力された処理ブロック入力データECに対してECB処理として復号化処理を行い、得られた暗号処理データPDを出力する。第4のセレクタは、排他的論理和演算器49が出力する排他的論理和データERを選択して、処理済データDCとして復号化結果を出力する。

【0081】

2) 56ビット鍵モードであり、かつ、CBCモードの定常状態である場合(図4のDEC-CBC Normalの場合)

この場合は、図3の下段の処理D2又はD3及びこれらのそれぞれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック4は、暗号化データCを入力とし、「Decrypt」処理を行って、データIを求める。暗号モード共用処理ブロック4は、求められたデータIとその前のECB処理で用いた暗号化データCとの排他的論理和を求めて、暗号化されていないデータDとして出力する。

【0082】

この場合の処理を、図2を参照して説明する。暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCBCモードの定常状態であることを示す信号が入力される。

【0083】

第1のセレクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセレクタ42は、遅延器48が出力する遅延された処理ブロック入力データECDを選択して出力する。排他的論理和演算器49は、暗号処理データPDと遅延された処理ブロック入力データECDとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

【0084】

第3のセレクタ43は、処理ブロック入力データECを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

【0085】

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセレクタから出力された処理ブロック入力データECに対してECB処理として復号化処理を行い、得られた暗号処理データPDを出力する。第4のセレクタは、排他的論理和演算器49が出力する排他的論理和データERを選択して、処理済データDCとして復号化結果を出力する。

【0086】

3) 56ビット鍵モードではなく、かつ、CBCモードの初期状態である場合
4) 56ビット鍵モードではなく、かつ、CBCモードの定常状態である場合
これらの場合は、それぞれ1), 2)の場合と次の点を除いて同じである。すなわち、暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードではないことを示す信号が入力される。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードではないことを示す信号が入力されているので、入力された56ビットの鍵データKDのうち、必要がないビット

(例えば上位16ビット)をマスクして、40ビット鍵データとしてECB処理器47に出力する。ECB処理器47は、ビットマスク器46から出力された40ビット鍵データを用いてECB処理を行う。

【0087】

5) 56ビット鍵モードであり、かつ、CFBモードの初期状態である場合(図4のDEC-CFB Initの場合)

CFBモードの処理のみを行うときには、CFBモードの初期状態における処理が行われる。この場合は、図3の下段の処理D9及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック4は、暗号化データCを入力とし、「Encrypt」処理を行って、データIを求める。暗号モード共用処理ブロック4は、求められたデータIと入力された初期ベクタデータIVデータとの排他的論理和を求めて、暗号化されていないデータDとして出力する。

【0088】

この場合の処理を、図2を参照して説明する。暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCFBモードの初期状態であることを示す信号が入力される。

【0089】

第1のセクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセクタ42は、初期ベクタデータIVを選択して出力する。排他的論理和演算器49は、暗号処理データPDと初期ベクタデータIVとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

【0090】

第3のセクタ43は、処理ブロック入力データECを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

【0091】

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データ

を用いて、第3のセレクタから出力された処理ブロック入力データECに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4のセレクタは、排他的論理和演算器49が出力する排他的論理和データERを選択して、処理済データDCとして復号化結果を出力する。

【0092】

6) 56ビット鍵モードであり、かつ、CFBモードの定常状態である場合（図4のDEC-CFB Normalの場合）

CBCモードの処理に続いてCFBモードの処理を行うときには、CFBモードの定常状態における処理が行われる。この場合は、図3の下段の処理D9及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック4は、その前のECB処理で用いた暗号化データCを入力とし、「Encrypt」処理を行って、データIを求める。暗号モード共用処理ブロック4は、求められたデータIと次の暗号化データCとの排他的論理和を求めて、暗号化されていないデータDとして出力する。

【0093】

この場合の処理を、図2を参照して説明する。暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCFBモードの定常状態であることを示す信号が入力される。

【0094】

第1のセレクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセレクタ42は、処理ブロック入力データECを選択して出力する。排他的論理和演算器49は、暗号処理データPDと処理ブロック入力データECとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

【0095】

第3のセレクタ43は、遅延器48が出力する遅延された処理ブロック入力データECDを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB

処理器 4 7 に出力する。

【0 0 9 6】

E C B 処理器 4 7 は、ビットマスク器 4 6 から出力された 5 6 ビット鍵データを用いて、第 3 のセクタから出力された遅延された処理ブロック入力データ E C D に対して E C B 処理として暗号化処理を行い、得られた暗号処理データ P D を出力する。第 4 のセクタは、排他的論理和演算器 4 9 が出力する排他的論理和データ E R を選択して、処理済データ D C として復号化結果を出力する。

【0 0 9 7】

7) 5 6 ビット鍵モードではなく、かつ、C F B モードの初期状態である場合
8) 5 6 ビット鍵モードではなく、かつ、C F B モードの定常状態である場合
これらの場合は、それぞれ 5), 6) の場合と次の点を除いて同じである。すなわち、暗号モード共用処理ブロック 4 には、モード選択信号 M S として、5 6 ビット鍵モードではないことを示す信号が入力される。ビットマスク器 4 6 は、モード選択信号 M S として 5 6 ビット鍵モードではないことを示す信号が入力されているので、入力された 5 6 ビットの鍵データ K D のうち、必要がないビット（例えば上位 1 6 ビット）をマスクして、4 0 ビット鍵データとして E C B 処理器 4 7 に出力する。E C B 処理器 4 7 は、ビットマスク器 4 6 から出力された 4 0 ビット鍵データを用いて E C B 処理を行う。

【0 0 9 8】

暗号モード共用処理ブロック 4 の暗号化処理時の動作について、図 2、図 3 の上段、及び図 4 を参照して説明する。この場合、暗号モード共用処理ブロック 4 には、暗号化／復号化切り替え信号 S S として、暗号化を示す信号が入力される。5 6 ビット鍵モードであるか否か、C B C モード及び C F B モードのうちのいずれであるか、初期状態及び定常状態のうちのいずれであるかによって場合を分けて説明する。E C B 処理器 4 7 における E C B 処理は、C B C モードの場合及び C F B モードの場合ともに暗号化処理である。

【0 0 9 9】

9) 5 6 ビット鍵モードであり、かつ、C B C モードの初期状態である場合（図 4 の E N C - C B C I n i t の場合）

この場合は、図3の上段の処理E1及びその前の排他的論理和を求める処理が行われる。暗号モード共用処理ブロック4は、入力された初期ベクタデータIVと暗号化されていないデータDとの排他的論理和を求めて、データIとして出力する。暗号モード共用処理ブロック4は、得られたデータIにECB処理として「Encrypt」処理を行って、暗号化データCを求めて出力する。

【0100】

この場合の処理を、図2を参照して説明する。暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCBCモードの初期状態であることを示す信号が入力される。

【0101】

第1のセレクタ41は、処理ブロック入力データECを選択して出力する。第2のセレクタ42は、初期ベクタデータIVを選択して出力する。排他的論理和演算器49は、処理ブロック入力データECと初期ベクタデータIVとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

【0102】

第3のセレクタ43は、排他的論理和データERを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

【0103】

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセレクタから出力された排他的論理和データERに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4のセレクタは、暗号処理データPDを選択して、処理済データDCとして暗号化結果を出力する。

【0104】

10) 56ビット鍵モードであり、かつ、CBCモードの定常状態である場合
(図4のENC-CBC Normalの場合)

この場合は、図3の上段の処理E2又はE3及びこれらのそれぞれの前の排他的論理和を求める処理が行われる。暗号モード共用処理ブロック4は、暗号化されていないデータDとその前のECB処理で得られた暗号化データCとの排他的論理和を求めて、データIとして出力する。暗号モード共用処理ブロック4は、得られたデータIにECB処理として「Encrypt」処理を行って、暗号化データCを求めて出力する。

【0105】

この場合の処理を、図2を参照して説明する。暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCBCモードの定常状態であることを示す信号が入力される。

【0106】

第1のセクタ41は、処理ブロック入力データECを選択して出力する。第2のセクタ42は、遅延器48が出力する遅延された暗号処理データPDDを選択して出力する。排他的論理和演算器49は、処理ブロック入力データECと遅延された暗号処理データPDDとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データERを出力する。

【0107】

第3のセクタ43は、排他的論理和データERを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

【0108】

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセクタから出力された排他的論理和データERに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4のセクタは、暗号処理データPDを選択して、処理済データDCとして暗号化結果を出力する。

【0109】

11) 56ビット鍵モードではなく、かつ、CBCモードの初期状態である場

合

12) 56ビット鍵モードではなく、かつ、CBCモードの定常状態である場合

これらの場合は、それぞれ9), 10) の場合と次の点を除いて同じである。すなわち、暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードではないことを示す信号が入力される。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードではないことを示す信号が入力されているので、入力された56ビットの鍵データKDのうち、必要がないビット(例えば上位16ビット)をマスクして、40ビット鍵データとしてECB処理器47に出力する。ECB処理器47は、ビットマスク器46から出力された40ビット鍵データを用いてECB処理を行う。

【0110】

13) 56ビット鍵モードであり、かつ、CFBモードの初期状態である場合(図4のENC-CFB Initの場合)

CFBモードの処理のみを行うときには、CFBモードの初期状態における処理が行われる。この場合は、図3の上段の処理E9及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック4は、暗号化されていないデータDを入力とし、「Encrypt」処理を行う。暗号モード共用処理ブロック4は、この処理で求められたデータと入力された初期ベクタデータIVデータとの排他的論理和を求めて、暗号化データCとして出力する。

【0111】

この場合の処理を、図2を参照して説明する。暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCFBモードの初期状態であることを示す信号が入力される。

【0112】

第1のセクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセクタ42は、初期ベクタデータIVを選択して出力する。排他的論理和演算器49は、暗号処理データPDと初期ベクタデータIVとの排他的論理和を対応するビット毎に求め、得られた排他的論理和データER

を出力する。

【0113】

第3のセクタ43は、処理ブロック入力データECを選択してECB処理器47に出力する。ビットマスク器46は、モード選択信号MSとして56ビット鍵モードであることを示す信号が入力されているので、入力された56ビットの鍵データKDをマスクせずにそのままECB処理器47に出力する。

【0114】

ECB処理器47は、ビットマスク器46から出力された56ビット鍵データを用いて、第3のセクタから出力された処理ブロック入力データECに対してECB処理として暗号化処理を行い、得られた暗号処理データPDを出力する。第4のセクタは、排他的論理和演算器49が出力する排他的論理和データERを選択して、処理済データDCとして暗号化結果を出力する。

【0115】

14) 56ビット鍵モードであり、かつ、CFBモードの定常状態である場合(図4のENC-CFB Normalの場合)

CBCモードの処理に続いてCFBモードの処理を行うときには、CFBモードの定常状態における処理が行われる。この場合は、図3の上段の処理E9及びこれに続く排他的論理和を求める処理が行われる。暗号モード共用処理ブロック4は、その前のECB処理で得られた暗号化データCを入力とし、「Encrypt」処理を行う。暗号モード共用処理ブロック4は、この処理で求められたデータと暗号化されていないデータDとの排他的論理和を求めて、暗号化データCとして出力する。

【0116】

この場合の処理を、図2を参照して説明する。暗号モード共用処理ブロック4には、モード選択信号MSとして、56ビット鍵モードであること、及びCFBモードの定常状態であることを示す信号が入力される。

【0117】

第1のセクタ41は、ECB処理器47が出力する暗号処理データPDを選択して出力する。第2のセクタ42は、処理ブロック入力データECを選択し

て出力する。排他的論理和演算器 49 は、暗号処理データ PD と処理ブロック入力データ EC との排他的論理和を対応するビット毎に求め、得られた排他的論理和データ ER を出力する。

【0118】

第 3 のセクタ 43 は、遅延器 48 が出力する遅延された暗号処理データ PDD を選択して ECB 処理器 47 に出力する。ビットマスク器 46 は、モード選択信号 MS として 56 ビット鍵モードであることを示す信号が入力されているので、入力された 56 ビットの鍵データ KD をマスクせずにそのまま ECB 処理器 47 に出力する。

【0119】

ECB 処理器 47 は、ビットマスク器 46 から出力された 56 ビット鍵データを用いて、第 3 のセクタから出力された遅延された暗号処理データ PDD に対して ECB 処理として暗号化処理を行い、得られた暗号処理データ PD を出力する。第 4 のセクタは、排他的論理和演算器 49 が出力する排他的論理和データ ER を選択して、処理済データ DC として暗号化結果を出力する。

【0120】

15) 56 ビット鍵モードではなく、かつ、CFB モードの初期状態である場合

16) 56 ビット鍵モードではなく、かつ、CFB モードの定常状態である場合

これらの場合は、それぞれ 13), 14) の場合と次の点を除いて同じである。すなわち、暗号モード共用処理ブロック 4 には、モード選択信号 MS として、56 ビット鍵モードではないことを示す信号が入力される。ビットマスク器 46 は、モード選択信号 MS として 56 ビット鍵モードではないことを示す信号が入力されているので、入力された 56 ビットの鍵データ KD のうち、必要がないビット（例えば上位 16 ビット）をマスクして、40 ビット鍵データとして ECB 処理器 47 に出力する。ECB 処理器 47 は、ビットマスク器 46 から出力された 40 ビット鍵データを用いて ECB 処理を行う。

【0121】

なお、モード選択信号MSがECBモードを示す場合には、第3のセクタ43は処理ブロック入力データECを選択して出力し、かつ、第4のセクタ44は暗号処理データPDを選択して出力する。ECB処理器47は、暗号化／復号化切り替え信号SSが、暗号化を示す場合は暗号化処理を行い、復号化を示す場合は復号化処理を行う。すなわち、図1の暗号化復号化装置は、CBCモード及びCFBモードに加えてECBモードにおける暗号化及び復号化を行うことができる。

【0122】

また、56ビット鍵データ又は40ビット鍵データに代えて、他の長さの鍵データを用いるようにすることも容易にできる。

【0123】

また、図1の暗号化復号化装置を暗号化装置として用いるようにしてもよい。この場合は、入力されたダウンストリームデータを暗号化して出力するのみでよく、以上の説明における復号化に対応した構成及び動作は不要である。また、暗号化／復号化切り替え信号SSは不要であり、第1～第4のセクタ及びECB処理器は、モード選択信号MSに従って動作すればよい。

【0124】

より具体的には、遅延器は、暗号処理データPDを入力とし、これを遅延させて出力する。第2のセクタは、処理ブロック入力データEC、初期ベクタデータIV、及び遅延器が出力する遅延した暗号処理データPDDのうちのいずれかを選択して出力する。第3のセクタは、処理ブロック入力データEC、排他的論理和演算器が出力する排他的論理和データER、及び遅延した暗号処理データPDDのうちのいずれかを選択して出力する。第4のセクタは、暗号処理データPD及び排他的論理和データERのうちのいずれかを選択して、暗号化結果として出力する。

【0125】

また、図1の暗号化復号化装置を復号化装置として用いるようにしてもよい。この場合は、入力されたアップストリームデータを復号化して出力するのみでよく、以上の説明における暗号化に対応した構成及び動作は不要である。このため

、暗号処理データ P D を常に出力する第 1 のセクタ、及び排他的論理和演算器が出力する排他的論理和データ E R を常に出力する第 4 のセクタは不要である。また、暗号化／復号化切り替え信号 S S は不要であり、第 2 及び第 3 のセクタ及び E C B 処理器は、モード選択信号 M S に従って動作すればよい。

【 0 1 2 6 】

より具体的には、遅延器は、処理ブロック入力データ E C を入力とし、これを遅延させて出力する。第 2 のセクタは、処理ブロック入力データ E C、初期ベクタデータ I V、及び遅延器が出力する遅延した処理ブロック入力データ E C D のうちのいずれかを選択して出力する。第 3 のセクタは、処理ブロック入力データ E C、及び遅延した処理ブロック入力データ E C D のうちのいずれかを選択して出力する。排他的論理和演算器は、暗号処理データ P D と第 2 のセクタの出力との排他的論理和を求めて、復号化結果として出力する。

【 0 1 2 7 】

また、本発明は、C P U や D S P (digital signal processor) 等のプロセッサを用いたソフトウェアによる処理を行うことによって実現することも可能である。

【 0 1 2 8 】

以上のように、本発明に係る暗号化復号化装置によると、モード選択信号を変化させれば、E C B モード、C B C モード及び C F B モードのうちのいずれかと、5 6 ビット鍵モード又は 4 0 ビット鍵モードのいずれかとを組み合わせたいずれのモードにおいても、同一のハードウェアによって暗号化データに対する復号化を行い、暗号解読データを得ることができる。

【 0 1 2 9 】

また、暗号化／復号化切り替え信号を変化させれば、いずれのモードにおいても、データの暗号化及び復号化のいずれをも、同一のハードウェアによって行うことができる。

【 0 1 3 0 】

また、以上の暗号化／復号化をソフトウェアによって行う場合も、前記組み合わせのいずれのモードにおいても同一のソフトウェアによって暗号化及び復号化

を行うことができる。

【0131】

【発明の効果】

以上のように、本発明によると、同一のハードウェアによって多くのモードにおいて暗号化／復号化を行うことができるので、回路面積を削減してコストを抑えることができる。ソフトウェアによって実現する場合においても、プログラムの簡略化等を図ることができる。多くの機能を低コストで提供することができるので、コストパフォーマンスを高めることができる。

【図面の簡単な説明】

【図1】

本発明の実施形態に係る暗号化復号化装置の構成を示すブロック図である。

【図2】

図1の暗号モード共用処理ブロックの構成の例を示すブロック図である。

【図3】

図1の暗号モード共用処理ブロックが行う処理の流れを示す説明図である。

【図4】

図1の暗号モード共用処理ブロックの第1～第4のセレクタが選択するデータの組み合わせを示す説明図である。

【符号の説明】

- 2 データ構造解析ブロック
- 4 暗号モード共用処理ブロック
- 6 データ制御ブロック
- 41 第1のセレクタ
- 42 第2のセレクタ
- 43 第3のセレクタ
- 44 第4のセレクタ
- 46 ビットマスク器
- 47 ECB処理器
- 48 遅延器

49 排他的論理和演算器

SD ダウンストリームデータ

SU アップストリームデータ

TK TEK制御用データ

EC 処理ブロック入力データ

SS 暗号化／復号化切り替え信号

MS モード選択信号

IV 初期ベクタデータ

KD 鍵データ

PD 暗号処理データ

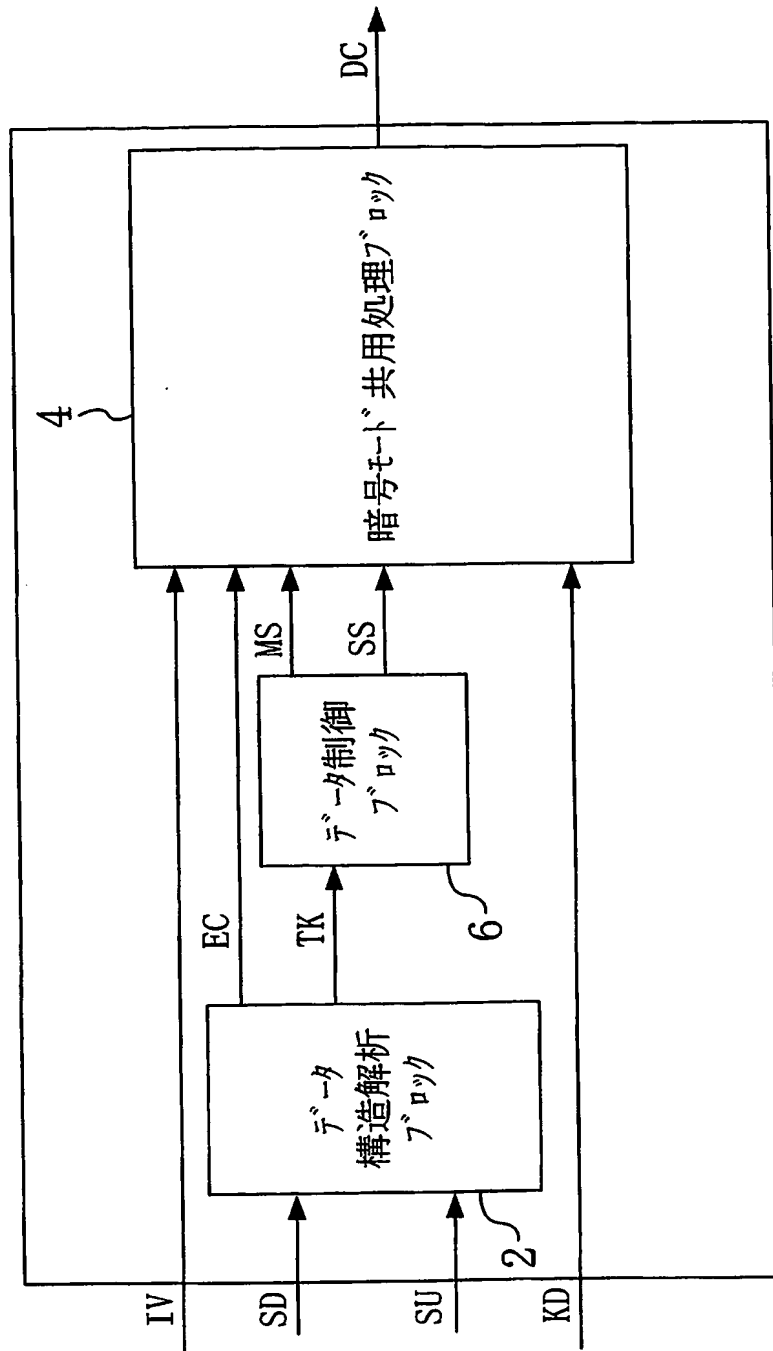
ECD 遅延した処理ブロック入力データ

PDD 遅延した暗号処理データ

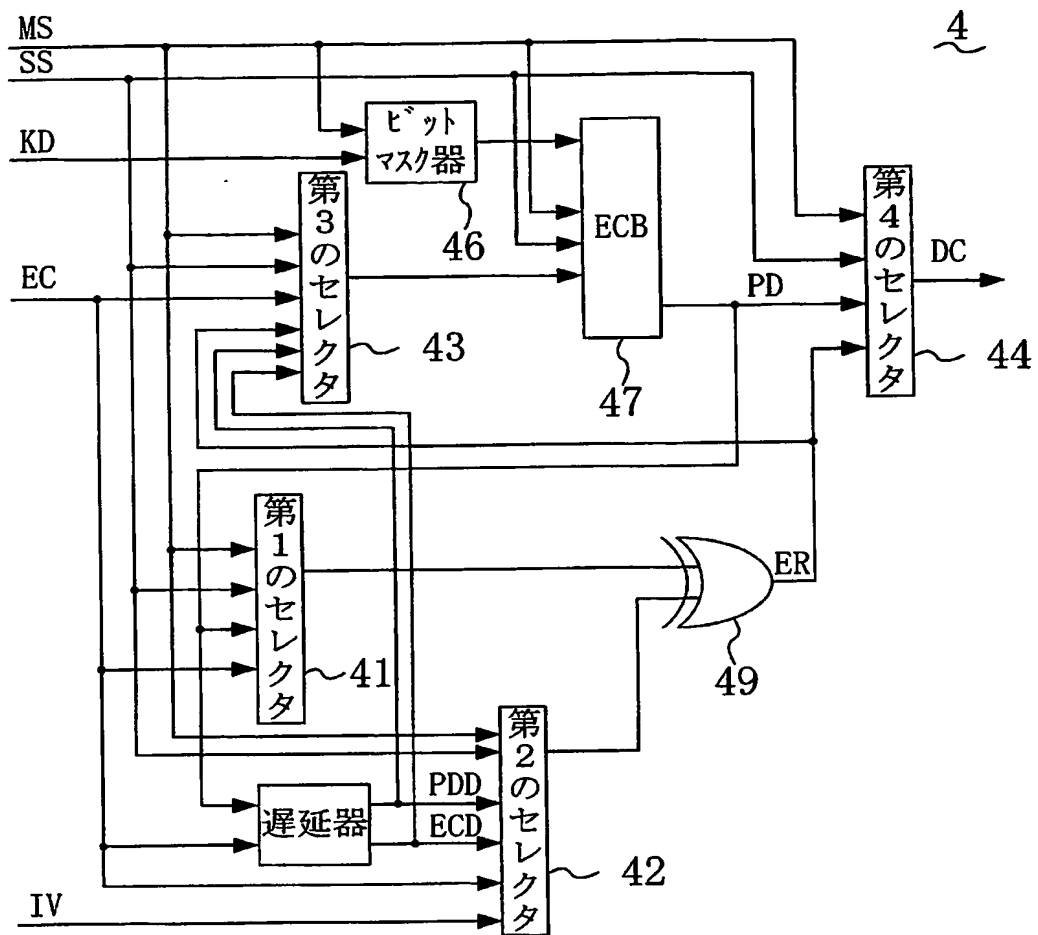
【書類名】

図面

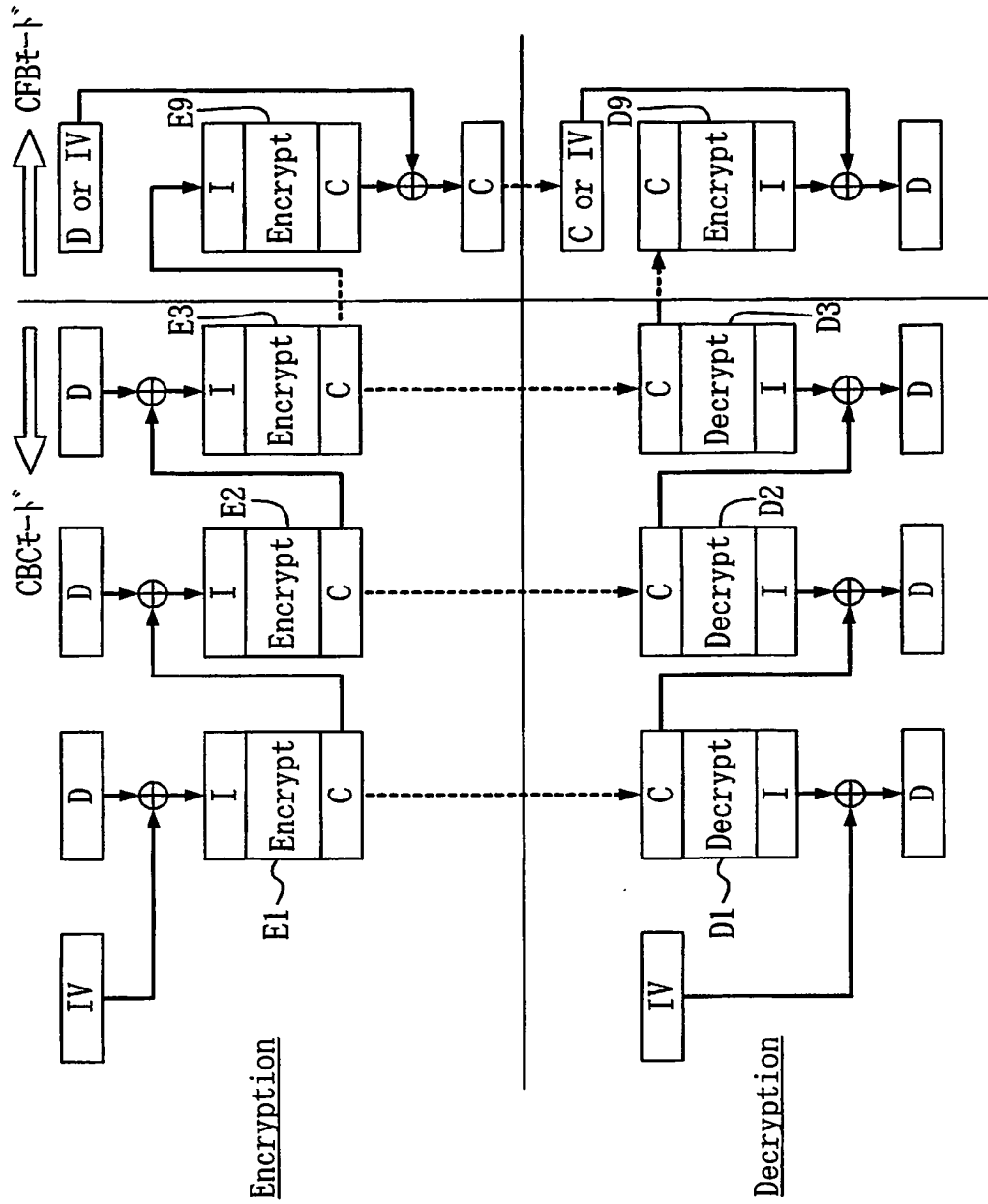
【図 1】



【図 2】



【図 3】



【図 4】

	DEC-CBC Init	DEC-CBC Normal	DEC-CFB Init	DEC-CFB Normal	ENC-CBC Init	ENC-CBC Normal	ENC-CFB Init	ENC-CFB Normal
第1のレクタ	PD	PD	PD	PD	EC	EC	PD	PD
第2のレクタ	IV	ECD	IV	EC	IV	PDD	IV	EC
第3のレクタ	EC	EC	EC	ECD	ER	ER	EC	PDD
第4のレクタ	ER	ER	ER	ER	PD	PD	ER	ER

【書類名】 要約書

【要約】

【課題】 複数のモードで処理回路を共用化して、回路規模を削減する。

【解決手段】 暗号化復号化装置として、暗号化データを含むダウンストリームデータ又は暗号化すべきデータを含むアップストリームデータを受け取り、TEK制御用データ、及び、暗号化データ又は暗号化すべきデータを処理ブロック入力データとして出力するデータ構造解析ブロックと、TEK制御用データに従ってモード選択信号を求めて出力するデータ制御ブロックと、処理ブロック入力データに対して暗号化又は復号化を行い、得られた結果を出力する暗号モード共用処理ブロックとを備える。暗号モード共用処理ブロックは、入力された鍵データを用いたECB処理を行うことによって、CBCモード及びCFBモードのいずれにおいても暗号化及び復号化を行うことができるように構成されており、モード選択信号に示されたモードで暗号化又は復号化を行う。

【選択図】 図1

特願 2 0 0 2 - 2 3 1 2 8 4

出 願 人 履 歷 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☒ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.